Analysis of Security Certificates

Denis Varga, Roman Oravec, Samuel Obuch

SLS 32TLC00xS(M) CIPURSE™4move v1.00.00

Description

- Evaluation Assurance Level EAL 5
- Smartcard device
- Software part compliant to CIPURSE™V2
- Connected to a terminal via contactless interface
- Contactless ticketing / payment applications

Not in scope

- Optionally available symmetric crypto library
- Configuration of access rights, secure messaging rules, file content and AES keys
- Terminal support, the terminal shall ensure integrity and confidentiality of transferred data

Threats

- T.Access - Unallowed execution of commands / access of assets
- T.Access_UID - Access UID to link and trace user sessions
- T.Forge-Auth - Forge authentication data to obtain authorisation
- T.Hijack-Session - Hijack an authorised session (man-in-the middle or replay attack).
- T.Tearing - Create an inconsistent state within the TOE to compromise an asset

SARs and SFRs

- SARs entirely based on Part 3 of the Common Criteria
- SFRs selected from Common Criteria part 2
- TOE Security Functionality:
  SF.Authenticate, SF.SM, SF.Access, SF.Command-Atomicity, SF.NoTrace

Conclusions

- Rigorous testing
- Missing SARs conformance description
- Limited scope

NEXOR® Sentinel 3E Filtering System

Description

- The Target of Evaluation (TOE) is a portion of the Nexor Sentinel 3.3 high assurance mail guard, specifically the Filtering Engine.
- The TOE is used to prevent unintentional mistakes from users that violate organisational security policies.

Filters

- Dirty Word Searching Filter
- Allowed Attachment Types Filter
- Security Label for Domain Filter (Structured and unstructured)
- Filters can be configured by an administrator

Security assumptions

- The TOE shall be managed by workstations that cannot connect to un-trusted web servers (such as on the internet).
- Both administrators and those who send/receive messages through the TOE are trustworthy and will not abuse their privileges.
- The TOE shall provide a secure web-based interface that enables configuration of the filters.

Threats

- A member of the organisation accidentally sends an email with contents which should not be transferred from one domain to another.
- A member of the organisation accidentally sends an email from one domain to another that fails to include an appropriate security label.
- A member of the organisation accidentally sends an email from one domain to another containing one or more attachments of a type considered a security risk.
- A user who is not properly identified and authenticated as an administrator is able to make unauthorised changes to the TOE filter configuration.

SFRs and SARs

- All SFRs are from CC Part 2; there are no explicitly stated requirements.
- Most relevant SFRs for TOE functionality:
  - FDP_IFC.1 – Information flow control policy
  - FDP_IFF.1 – Information flow control functions
  - FIA_UAU.2 – User authentication before any action
- SARs of EAL4 from Part 3 of the CC
  - ALC_FLR.2 – assurance in flaw remediation process.

Infineon Technologies AG Trusted Platform Module SLB9665_2.0

Description

- integrated circuit and software platform
- basically a secure controller with following functionalities:
  - Random number generator
  - Cryptographic key generator
  - Symmetric and asymmetric key procedures
  - Hash algorithms
  - Secure key and data storage
  - Identification and Authorization mechanism

Security assumptions and attacker threats

- Assumptions:
  - assumed to be in an uncontrolled environment with no guarantee of its physical security.
  - must be installed and configured properly
  - must create EK and AK credentials by trustworthy procedures
  - …
- Threats:
  - undetected compromise of the data in shielded locations
  - unauthorised individual may impersonate an authorised user
  - originator of data may deny originating the data to avoid accountability
  - …

SARs and SFRs

- Security assurance requirements:
  - as defined in Common Criteria part 3 and augmented with ALC_FLR.1 and AVA_VAN.4
- Security functional requirements:
- Selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended
  - Cryptographic Support
  - Identification and Authentication
  - General and Test
  - Object Hierarchy
  - TOE Operation

Evaluations

- Developer tests:
  - developer tests cover all security functionalities and all security mechanisms as identified in the functional specification
- Evaluator tests:
  - evaluators were able to repeat the tests of the developer, either using the tools and TOE samples delivered to the evaluator, or at the developer's site.
- evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer.
- cryptographic algorithms was not rated
- Penetration tests

Conclusion

- Large quantity of tests
- Multiple documents and added specification
- Also has guidelines on product identification and shipment
- Widely used, prone to more attacks